AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of New York

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

THE PREMISES KNOWN AND DESCRIBED AS AN LG MOBILE PHONE BEARING SERIAL NUMBER 803CYEA327740, CURRENTLY LOCATED AT 335 ADAMS STREET, 32ND FLOOR, BROOKLYN, NY 11202

Case No. 20-M-153

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of New York
(identify the person or describe the property to be searched and give its location):

THE PREMISES KNOWN AND DESCRIBED AS AN LG MOBILE PHONE BEARING SERIAL NUMBER 803CYEA327740, CURRENTLY LOCATED AT 335 ADAMS STREET, 32ND FLOOR, BROOKLYN, NY 11202, AS SET FORTH IN ATTACHMENT A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

EVIDENCE, FRUITS AND INSTRUMENTALITIES OF VIOLATIONS OF FEDERAL OFFENSES, AS SET FORTH IN ATTACHMENT B.

YOU ARE COMMANDED to execute this warrant on or before February 28, 2020 *(not to exceed 14 days)*
☐ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the Duty Magistrate Judge.
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*
☐ for _____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 2/14/2020 @ 11:48a.m.

S/ Lois Bloom
Judge's signature

City and state: Brooklyn, New York

Hon. Lois Bloom U.S.M.J.
Printed name and title

Return

Case No.: 20-M-153	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

Description of the Property to Be Searched

The property to be searched is a LG K20 (M255) smartphone bearing serial number 803CYEA327740 and International Mobile Equipment Identity ("IMEI") number 355574-08-327740-5 (the "Device"). The Device is currently located at the USSS New York Field Office located at 335 Adams Street, 32nd Floor, Brooklyn, New York 11201.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Description of the Things to Be Seized

1. All records on the Device described in Attachment A that relate to violations of 18 U.S.C. §§ 115(a)(1)(A) and 875(c) and involve Frank Monte since June 1, 2019, including:

   a. records of incoming and outgoing calls;

   b. records, including text messages, web browser history and search terms, related to the President, any federal law enforcement officers, or federal facilities; and

   c. records reflecting the device's movements and location, including GPS location data.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as call logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

AB:ADG

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF AN LG MOBILE PHONE BEARING SERIAL NUMBER 803CYEA327740, CURRENTLY LOCATED AT 335 ADAMS STREET, 32ND FLOOR, BROOKLYN, NEW YORK 11202	APPLICATION FOR A SEARCH WARRANT FOR AN ELECTRONIC DEVICE Case No. 20-M-153

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, William Kirkland, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the United States Secret Service (the "USSS"), and have been since September 2017. I am currently assigned to the USSS Newark Field Office, located in Morristown, New Jersey (the "Morristown Field Office"). I am responsible for investigations of criminal violations related to financial institution fraud, credit card fraud, counterfeiting and threats against the President of the United States. I have received training in, and have participated in a number of investigations into threats to the President and other Federal officials, credit card fraud, counterfeiting and other types of bank fraud investigations, including participating in surveillance, arrests, search warrants and interviews. To support those

investigations, I have received training and gained experience in the review of electronic devices, including computers and mobile phones.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

4. The property to be searched is a LG K20 (M255) smartphone bearing serial number 803CYEA327740 and International Mobile Equipment Identity ("IMEI") number 355574-08-327740-5 (the "Device"). The Device is currently within the lawful possession of the USSS at the USSS New York Field Office located at 335 Adams Street, 32nd Floor, Brooklyn, New York 11201, in the Eastern District of New York.

5. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

6. The USSS is investigating Frank Monte ("Monte") for placing multiple telephone calls containing threats against Federal law enforcement officers at various times in or around July and October 2019, in violation of 18 U.S.C. §§ 115(a)(1)(B) (threats against a Federal law enforcement officer) and 875(c) (threats in interstate commerce). Monte is a veteran of the United States Navy. At times relevant to this investigation, Monte was a resident at various locations within New Jersey, including multiple facilities operated by the U.S. Department of Veterans Affairs (the "VA").

7. On or about July 17, 2019, a hearing took place at the VA campus in Lyons, New Jersey (the "Lyons Campus") to determine whether Monte should be subject to involuntary civil commitment for mental-health treatment. At that time, the USSS was already aware of Monte

given his criminal history, history of mental-health treatment and fixation on President Donald Trump. The USSS was also investigating Monte for other suspected criminal conduct. Victim-1, a USSS special agent, was assigned to that investigation.

8. Based on the USSS investigation into Monte and Monte's history of criminal conduct and mental-health treatment, Victim-1 testified at the July 17, 2019 hearing. Due to Victim-1's concern for personal safety and fear of reprisal by Monte, Victim-1 was permitted to identify during the hearing as "Special Agent #1" rather than Victim-1's actual name.

9. After the hearing, Monte remained involuntarily committed at the Lyons Campus from in or around July 2019 until in or around September 2019.

10. On or about July 21, 2019, Monte placed multiple harassing and threatening telephone calls to the emergency line of the VA Police station at the Lyons Campus. During one of those calls, Monte stated to Victim-2, a VA Police officer (and, therefore, a federal law enforcement officer): "I'm going to shoot you up."

11. On or about October 15, 2019, Monte placed a telephone call to a federal congressional office and spoke with a staff member there (the "October 15 Call"). During that call, Monte stated that if he "ever sees Special Agent #1 in New Jersey, he will knock him the fuck out."

12. On or about October 18, 2019, Monte placed a telephone call to a special agent of the U.S. Capitol Police, who had also been assigned to investigate Monte (the "October 18 Call"). During that call, Monte asked the Capitol Police special agent to come with Monte to Morristown, New Jersey—the location of the Morristown Field Office, to which Victim-1 was assigned at the time—to have a "conversation" with "Special Agent #1." Monte further stated, in sum and substance, that he was going to Morristown, that "it won't be much of a

conversation," and that he would drag "Special Agent #1" out from behind his desk, "kick his ass," and "put him in the hospital."

13. On October 30, 2019, U.S. Magistrate Judge Cathy Waldor of the District of New Jersey issued a criminal complaint against Frank Monte (Mag. No. 19-mj-7485-CLW). That complaint charged Monte with violating 18 U.S.C. §§ 115(a)(1)(B) and 875(c) by making the telephone calls described above. Judge Waldor also issued an arrest warrant for Monte on the same date.

14. On October 31, 2020, law enforcement officers arrested Monte pursuant to the October 30, 2020 arrest warrant. At that time, law enforcement officials took custody of various personal effects in Monte's possession, including the Device.

15. Shortly thereafter, law enforcement slid the unlocked back cover from the Device, revealing a label bearing the Device's IMEI number as "355574-08-327740-5."

16. On November 14, 2020, a grand jury in the District of New Jersey returned a five-count indictment against Monte based on the same underlying facts (Crim. No. 19-cr-821-ES).

17. Toll records obtained by law enforcement show that both the October 15 Call and the October 18 Call were placed from a device bearing the same device type (an LG-M255 smartphone) and IMEI number as the Device. Additionally, those records show that both the October 15 Call and the October 18 Call were placed from an originating number that the same records show was assigned to Monte. Accordingly, there is probable cause to believe that Monte used the Device to place both the October 15 Call and the October 18 Call and that the Device will contain records of those calls, as well as other records, including web browser history and search terms, that may relate to the subjects discussed on any of the calls referenced in this affidavit. Based on my experience and training, I also believe that the Device may contain

records that will tend to establish the geographic location of the phone's user during the October 15 Call and the October 18 Call, in a manner that may tend to establish, among other things, the interstate nature of the calls.

18. The Device is currently in storage at the USSS New York Field Office located at 335 Adams Street, 32nd Floor, Brooklyn, New York 11201. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of the USSS on October 31, 2019.

TECHNICAL TERMS

19. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also

include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists

of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

20. Based on my training, experience and research, and from consulting the manufacturer's advertisements and product technical specifications available online at www.lg.com/us/cell-phones/lg-M255-k20, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device and

PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

21. Based on my knowledge, training and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

22. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

23. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

24. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

25. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

S/ William Kirkland
William Kirkland
Special Agent
United States Secret Service

Subscribed and sworn to before me on February 14, 2020:

S/ Lois Bloom
THE HONORABLE LOIS BLOOM
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

Description of the Property to Be Searched

The property to be searched is a LG K20 (M255) smartphone bearing serial number 803CYEA327740 and International Mobile Equipment Identity ("IMEI") number 355574-08-327740-5 (the "Device"). The Device is currently located at the USSS New York Field Office located at 335 Adams Street, 32nd Floor, Brooklyn, New York 11201.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Description of the Things to Be Seized

1. All records on the Device described in Attachment A that relate to violations of 18 U.S.C. §§ 115(a)(1)(A) and 875(c) and involve Frank Monte since June 1, 2019, including:

   a. records of incoming and outgoing calls;

   b. records, including text messages, web browser history and search terms, related to the President, any federal law enforcement officers, or federal facilities; and

   c. records reflecting the device's movements and location, including GPS location data.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as call logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.